Amendments to the Claims

Claim 1 (currently amended): A computer-implemented method of providing cross-domain authentication in a computing environment, comprising ~~steps of~~:

providing security credentials of an entity to an initial point of contact that provides content aggregation in the computing environment;

passing the provided credentials from the initial point of contact to a local trust proxy in a local security domain of the initial point of contact;

authenticating the ~~passed credentials~~ entity with an authentication service in [[a]] the local security domain, using the passed credentials, ~~of the trust proxy to authenticate the entity~~ for accessing content from at least one local content service, each of the at least one local content services operable to provide its content from the local security domain for aggregation, by the initial point of contact, in an aggregated view;

responsive to a successful outcome of the authenticating, forwarding an authentication assertion for the successful outcome to a remote trust proxy in each of at least one selected remote security domains, the authentication assertion comprising an identification of the entity;

using the identification from the authentication assertion, by the remote trust proxy in each of the at least one selected remote security domains, to locate previously-stored security credentials usable for authenticating the entity in that remote security domain, wherein the located security credentials usable for authenticating the entity in at least one of the selected remote security domains differ from the security credentials of the entity provided to the initial point of contact; and

authenticating the entity with an authentication service in each of the at least one selected

remote security domains, using the located security credentials usable for authenticating the entity in that remote security domain, ~~authentication performed by the local authentication service to seamlessly authenticate the entity~~ for accessing other content from at least one remote content service that is operable in that ~~each of at least one selected~~ remote security ~~domains~~ domain[[,]] ~~each of the at least one remote content services operable~~ to provide its content from that [[its]] remote security domain for aggregation, by the initial point of contact, in the aggregated view.

Claim 2 (currently amended): The method according to Claim 1, wherein the ~~using step~~ forwarding further comprises ~~the steps of:~~

~~———~~consulting policy information to determine which of a plurality of remote security domains should be selected as the at least one selected remote security ~~domain; and~~

~~———passing the information from the local authentication service to each of the determined remote security~~ domains.

Claim 3 (currently amended): The method according to Claim 1, wherein the using [[step]] the identification to locate previously-stored security credentials and the authenticating the entity using the located security credentials enable accessing the other content from ~~enables each of~~ the remote content services in the selected remote security domains ~~to be accessed by the entity~~ without requiring the entity to provide [[its]] the previously-stored security credentials ~~for those remote content services~~ to the initial point of contact.

Claim 4 (canceled)

Claim 5 (original): The method according to Claim 1, wherein the entity is an end user.

Claim 6 (original): The method according to Claim 1, wherein the initial point of contact is a portal interface.

Claim 7 (currently amended): The method according to Claim 1, wherein the passing [[step]] is performed by a proxy of the initial point of contact.

Claim 8 (currently amended): The method according to Claim 7, wherein the proxy of the initial point of contact performs a protocol conversion, when passing the provided credentials, from a first protocol used in the providing [[step]] to a second protocol used by the trust proxy.

Claim 9 (original): The method according to Claim 8, wherein the first protocol is Hypertext Transfer Protocol ("HTTP") or a security-enhanced version thereof.

Claim 10 (original): The method according to Claim 8, wherein the second protocol is Simple Object Access Protocol ("SOAP").

Claim 11 (canceled)

Claim 12 (currently amended): The method according to Claim 1, ~~wherein the using step~~ further

~~comprises the steps of:~~ comprising forwarding the authentication assertion, by the remote trust proxy in each of the at least one selected remote security domains, to the authentication service in that remote security domain, which relies on the forwarded authentication assertion when authenticating the entity using the located security credentials.

~~forwarding a security token from the local authentication service to a remote trust proxy in each of the selected remote security domains; and~~

~~using the forwarded security token, at each of the remote trust proxies, to authenticate the entity with an authentication service in the remote security domain.~~

Claim 13 (currently amended): The method according to Claim 12, wherein the successful outcome ~~results~~ of the authenticating ~~authentication by the authentication service~~ in the local security domain and results of the authenticating ~~each authentication by the authentication services~~ in each of the selected remote security ~~domain~~ domains are returned to the initial point of contact for use when creating the aggregated view.

Claim 14 (currently amended): The method according to Claim 13, further comprising using the returned successful outcome and the returned results of the authenticating in each of the selected remote security domains to determine, ~~the step of determining,~~ by the initial point of contact, which of the content and the other content can be aggregated by the initial point of contact ~~based on the returned results~~ in the aggregated view.

Claim 15 (canceled)

Claim 16 (currently amended): A system for enabling an entity to have seamless access to a plurality of aggregated services which have different identity requirements, comprising:

at least one computer, each comprising a processor; and

instructions which execute on at least one of at least one computers, using the processor of the computer, to implement functions comprising:

~~means for~~ initially authenticating the entity, by a first authentication component in a local security domain, for access to a first service in the local security domain using an identity provided by the entity using an aggregation interface in the local security domain;

~~means for~~ mapping the provided ~~identification~~ identity, in each of at least one remote security domains, to the ~~differing~~ different identity requirements of at least one other service which is provided by that remote security domain and which is to be aggregated with the first service, thereby establishing mapped identity requirements for each of the at least one other services;

~~means for~~ subsequently authenticating the entity, by an authentication component in each of the at least one remote security domains, for access to each of the at least one other services which is provided by that remote security domain, ~~by an authentication component associated with that other service,~~ using the mapped identity requirements; and

~~means for~~ aggregating each of the at least one other services and the first service, if the authentications thereof are successful, into an aggregated result accessible from the aggregation interface in the local security domain.

Claim 17 (original): The system according to Claim 16, wherein the aggregated result is an aggregated view.

Claim 18 (original): The system according to Claim 16, wherein the entity is a programmatic entity.

Claim 19 (currently amended): A computer program product for providing federated identity management within a distributed content aggregation framework, the computer program product embodied on one or more ~~computer-readable~~ computer-usable storage media and comprising computer-usable program code for:

~~computer-readable program code for~~ providing, to the content aggregation framework by a using entity, initial identity information that identifies the using entity for accessing a first content source that is operable within a first security domain in which the content aggregation framework is operable;

~~computer-readable program code for~~ authenticating the using identity, using the initial identity information, by a first authentication service in the first security domain;

~~computer-readable program code for~~ conveying results of the authentication by the first authentication service to at least one selected other authentication service, each of which is associated with a remote security domain that is distinct from the first security domain, along with the initial identity information;

using, in each remote security domain, the conveyed initial identity information to locate previously-stored identity information usable for authenticating the using identity in the remote

security domain;

~~computer-readable program code for~~ using the ~~conveyed results~~ located identity information, in each of the remote security domains, to authenticate the using entity to each of the selected other authentication services for accessing a remote content source operable within the remote security domain that is associated with that selected other authentication service, without requiring the using entity to provide ~~additional~~ the previously-stored identity information to the content aggregation framework; and

aggregating content from the first content source and other content from each of the remote content sources for presentation in an aggregated view rendered by the content aggregation framework.

Claim 20 (original): The computer program product according to Claim 19, wherein the initial identity information is a name and password associated with the using entity.

Claim 21 (currently amended): The method according to Claim 1, further comprising ~~the step of~~ rendering, by the initial point of contact, the aggregated view.